Rules of Behavior
Information Systems Security Principles

General Principles

The following principles of behavior apply to all users of the system whether Department of Justice (DOJ) employees or not. Because written guidance cannot cover every contingency, all individuals are asked to go beyond the stated principles, using their best judgement and highest ethical standards to guide actions. All individuals given access to DOJ automated information systems must understand that these principles are based on Federal laws, regulations and DOJ Orders. As such, there are consequences for non-compliance with principles of behavior. Whether the subject individual is a DOJ employee or not, management has the right to impose appropriate sanctions and/or cease the individual's access to computer systems.

I _______________________[*print name*] understand that when using DOJ automated IT systems, that I will be held accountable for my actions related to the information resources entrusted to me. I further understand the following items:

1. **Accountability:** Employees must be accountable for their actions and responsibilities related to information resources entrusted to them.

2. **Confidentiality:** Employees must protect sensitive information from disclosure to unauthorized individuals or groups.

3. **Passwords and User IDs:** Employees must protect information security through effective use of User IDs and passwords. Each system user will be assigned a unique personal identifier and password that shall be used to establish all personal accounts and access privileges for the individual. Users should immediately change passwords that have been initialized by an administrator. Protect your passwords! Each system user must protect their ID and password. Sharing of identification and password is a violation of DOJ Order 2640.2D and other federal regulations governing the distribution and use of User Identifications and Passwords, i.e., FIPS PUB 112. Also, users are prohibited from establishing a computer work session then allowing another person to "take their place" at the system.

4. **Hardware:** Employees must protect computer equipment from damage, abuse, and unauthorized use. This includes DOJ owned portable computers used for business while on travel or at place of residence.

5. **Reporting:** Employees must report security violations and vulnerabilities to their office's District Office Security Manager (DOSM) and Systems Manager. DOJ Security Guidance TP-001 (http"//10.173.2.12/jomd/css/dojcert/sop.htm) provides guidance for reporting

violations.

6. **Privileged Users:** Privileged users must perform their duties meticulously and reliably in order to preserve information security. Privileged users include: System Managers; computer operators; system engineers (those with control of the operating system); network administrators; those who have access to change control parameters for equipment and software; database administrators; those who control user passwords and access levels; and troubleshooters/system maintenance personnel.

7. **Work at Home And Other Remote Users:** Remote users must establish security standards at their workplace sufficient to protect hardware, software, and information. This includes having only those resources you really need and have authority to use; establishing a thorough understanding and agreement with your supervisor as to what your security responsibilities are; using software according to licensing agreements; ensuring that sensitive information that is downloaded is properly safeguarded, and that dial-in access is secure; and being alert for anomalies and vulnerabilities, reporting these to their District Office Security Manager and Systems Manager, and seeking advice when necessary. Work at home users may not use personally-owned hardware, software, or network connectivity for any work purposes.

8. **Users of Personal Information:** Users must acquire and use personal information only in ways that respect an individual's privacy. This includes: properly destroying personal information contained in hard copy or electronic format; and ensuring that personal information is accurate, timely, complete, and relevant for the purpose which it is collected, provided, and used.

Information Systems Security Rules

These rules of behavior are based on the general principles of behavior.

1. **Official Business**

   a. Do not steal hardware, software, information, or equipment.
   b. Do not develop computer programs for non-work purposes.
   c. Limit use of the computer for non-work purposes to non-business hours.

   [Justice Property Management Regulation (JPMR), 41 CFR pt 28 allows personal use of government equipment, as long as there is negligible cost to the department and it does not interfere with official business. Furthermore, the regulation goes on to state: "In using government property, employees should be mindful of their responsibilities to protect and conserve such property **and to use official time in an honest effort to perform official duties**." (Emphasis added).

2. **Access**

a. Only use data for which you have been granted authorization.
b. Do not retrieve information from a system for someone who does not have authority to access the information. Only give information to people who have access authority and who need the information for their jobs.
c. Abide by procedures governing the channels for requesting/disseminating information.
d. Limit the number of people who can access your files/data.
e. Do not access external computer systems (such as bulletin boards) unless necessary to perform an official duty.
f. Do not attempt to gain access to information to which you do not have authority.
g. Use access control features such as screen saver passwords and password protect highly sensitive files.

3. **Integrity**

a. Disconnect any networked system that shows indications of being infected with a virus. Discontinue use of any software or data files that are known or suspected of being infected with a virus.
b. Protect against viruses and similar malicious programs. Use only authorized software; do not use shareware, freeware, public domain software, or similar programs unless they are authorized.
c. Never enter unauthorized, inaccurate, or false information.
d. Do not manipulate information inappropriately.
e. Create only authorized records or files.
f. Scan all files and disks for viruses before use, especially if they are received from external sources.

4. **Availability**

a. Plan for contingencies such as disaster, loss of information, and disclosure of information by preparing alternate work strategies and recovery mechanisms.
b. Make backups of hard drive files on a regular basis.
c. Protect backups against being over-written.
d. Store backups away from the originals, in a physically separate location.
e. Keep storage media away from devices that produce magnetic fields.
f. Protect systems and media from food and drink spills.

5. **Hardware/Software**

a. Do not check laptops on airlines.

b. Safeguard computer equipment against damage, waste, loss, abuse, unauthorized use, and misappropriation.
c. Only use equipment for which you have been granted authorization.
d. Do not eat, drink, or smoke near computer equipment and media.
e. Do not store combustible materials near a computer.
f. Do not remove a PC or other computer hardware from EOUSA/USAO premises without a property pass.
g. Only remove computer equipment from EOUSA/USAO premises for official purposes.
h. Do not allow someone to perform maintenance without proper identification.
i. Only use software for which you have been granted authorization and have appropriate licenses.
j. Do not install any software, to include, unauthorized or public domain software without the approval of your Systems Manager.

6. **Reporting**

Report all security violations, incidents, and vulnerabilities to your office's District Office Security Manager (DOSM) and Systems Manager.

7. **Privileged Users**, e.g., Systems Managers, Case Managers, Database Administrators, Systems Engineers, etc.

a. Protect the privilege user passwords at highest level demanded by the sensitivity level of the system.
b. Report all security violations, incidents, and vulnerabilities to your office's DOSM (District Office Security Managers) and the EOUSA Information Systems Security Officer (ISSO).
c. All security incidents regarding loss or theft must also be reported to the EOUSA Security Programs Manager (SPM).
d. All security incidents regarding National Security Information must also be reported to the EOUSA Security Programs Manager (SPM).
e. File software licensing agreement with vendor within five days of receipt. Agreement must be signed and must include the registration number. Keep a copy of all licensing agreements.
f. Do not develop programs for non-work purposes.
g. Keep an inventory of all computer equipment and software you have in your office.
h. Keep records of all maintenance.
i. Help train users on appropriate use and security of system.
j. Watch for unscheduled or unauthorized programs running on a recurring basis.
k. Track all security incidents occurring within your area of responsibility.

l. Take action to reduce damage caused by security incidents, as appropriate, e.g., lock up property, log off of a terminal, and disconnect a PC with a virus from the LAN.

m. Establish security measures to ensure integrity, privacy, and availability of information on publicly accessible systems.

8. **Users of Public Access Systems**, e.g., Internet, Court Systems, etc.

a. Do not transmit Limited Official Use or other sensitive information across public access systems, including the Internet.

b. Use virus protection software when receiving information from a public access system.

c. Ensure that information placed on a public access system presents a professional image.

d. Ensure that information placed on a public access system is up-to-date, accurate, and true.

e. Ensure that information placed on a public access system reflects the policies and positions of the EOUSA and DOJ.

f. Do not distribute or receive documents via public access systems in violation of copyright laws.

9. **Managers**

a. Notify your staff's Computer System Security POC and security personnel whenever an employee terminates or changes status.

b. Complete a Network Account Request form whenever an employee terminates or changes status.

c. Ensure continued availability of data when a employee terminates by assisting the ISO with completing the ***Departing Employees/Contractors/Volunteers EOUSA Automation Clearance Form*** on the last day the departing individual is in the office and by get key to encrypted files.

d. Counsel terminating employees on non-disclosure of confidentially-sensitive information.

e. Terminate access to information and computer systems immediately in the event of employee separation.

f. Escort employee off the premises when there is likelihood of sabotage, as with an unfriendly termination or separation.

g. Ensure employees get adequate and appropriate training to do their job.

I understand that EOUSA/USAO will regularly review system logs and conduct spot-checks to determine if I am complying with policies and controls placed on the use IT Resources.

I understand that I must acquire and use sensitive information only in accordance with established policies and procedures. This includes: properly destroying sensitive information contained in hardcopy or softcopy; ensuring that sensitive information is accurate, timely complete, and relevant for the purpose which it is collected, provided, and used.

I will comply with all copyright licenses associated with information systems.

I will comply with the personal use of government equipment in accordance with EOUSA/USAOs' policies and procedures.

I acknowledge receipt of and understand my responsibilities, and will comply with the rules of behavior delineated herein.

Signature Date